Multi-Layered Security Framework for Metro-Scale Wi-Fi Networks

A Security Whitepaper
January, 2004

Introduction: A Multi-Layered Approach to Security

Securing 802.11 wireless networks is a serious concern. Numerous observers have highlighted the potential vulnerabilities of standard 802.11 wireless networks.

From the outset, one of Tropos Networks' primary objectives has been to offer the highest levels of security. The company has created a multi-layered security framework that achieves robust 802.11 network security through time-tested and proven techniques. This unique approach leverages the higher layer intelligence of Tropos Wi-Fi cells to provide protection at multiple levels.

This white paper discusses the Tropos Networks security architecture. Our approach closely follows the strongest industry recommendations for securing wireless networks.

The Tropos Approach: Multi-Layered, Time-Tested, Standards-Based

Tropos Networks security elements extend industry best practices for securing wireless networks and wireless data. Tropos implements only those security algorithms that have been widely tested and verified. Tropos utilized several guidelines to craft its security approach:

1. ***Multi-layered***—Utilize multiple security mechanisms at several network layers to provide high levels of protection.
2. ***Time-tested and proven***—Utilize security techniques that are well-known and trusted.
3. ***Open, standards-based***—Integrate elements that have undergone extensive scrutiny by the security community and can offer users a strong degree of confidence in their implementation.
4. ***Upgradeable***—Because new security threats often emerge, any architecture must be upgradeable to eliminate future security holes.

Each of the advanced security techniques employed in the Tropos Networks security model satisfies these design criteria. Techniques, protocols and algorithms such as traffic filtering, WEP, AES, HTTPS, and VPNs have been employed for several years in various Internet applications. Leveraging the higher-layer intelligence of its products, Tropos combines the best Internet security techniques to offer a robust and multi-layered security framework. No other 802.11 networking product combines all these elements to offer the highest layers of protection.

The task of securing wireless networks can be divided into five challenges:

- ***Network access control through authentication***—Wireless network security begins with prohibiting access by unauthorized wireless devices.
- ***Protection of wired assets from malicious wireless clients***—Because the goal of a wireless network is to provide access to a network of wired devices (servers, printers, databases), a wireless network deployment must carefully protect those resources from malicious users.
- ***Protection of wireless clients from other malicious wireless clients***—Wireless clients must be protected both for their own sake and to prevent a permitted client from being used for access by an unauthorized client.
- ***Secure end-to-end transmission of sensitive data***—Because malicious users can sniff the airwaves, data traffic traveling over the wireless network must be shielded from eavesdroppers by a strong encryption algorithm.
- ***Secure network configuration and management***—To prohibit sophisticated hacking, it should not be possible for anyone but authorized network operators to alter the operation of network elements or the network's path selection protocol.

The Tropos Networks Architecture

A Tropos network consists of a collection of Tropos 5110 and Tropos 3110 Wi-Fi cells. The Wi-Fi cells provide 802.11b wireless connectivity to end-user devices such as laptop computers and PDAs. They also provide high performance IP connections to servers or to devices on the wired network.

Each Tropos Wi-Fi cell that is configured as a gateway is connected to an Ethernet segment and provides a connection to a wired network. Wi-Fi cells configured as nodes dynamically forward end-user traffic along the best air-path available. A DHCP server located on one or more of the gateways in the network assigns IP addresses to all end-user devices as well as to the Wi-Fi cells themselves.

A simple diagram of a Tropos network is illustrated in Figure 1.

In the following sections, we will outline how the Tropos security tools operate in conjunction with our predictive path optimization and lightweight control protocol to secure the wireless network for even the most stringent operator requirements.

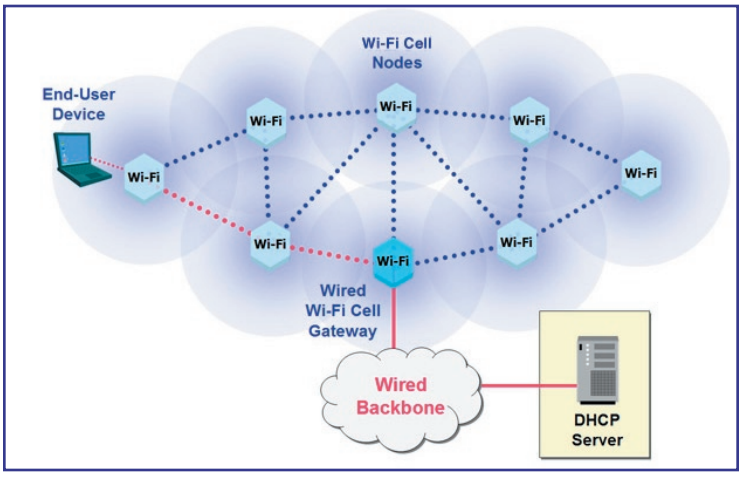


Figure 1: The Tropos Totally Wireless Network

Layer 2 Deterrents: WEP, MAC Address ACLs and ESSID Suppression

Layer 2 deterrents offer limited security. The techniques to overcome them are generally known and only a moderate amount of computational resource is required to break layer 2 deterrents. While layer 2 deterrents are useful as the first step in a comprehensive wireless security strategy, alone they cannot be relied upon to protect sensitive data.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the security measure incorporated into the 802.11 standard and can be considered as contributing to two aspects of wireless security, namely **network access control** and **secure data transmission**. By encrypting all wireless (802.11) frames using the same private key, WEP offers a mechanism that isolates usage of the network to authorized devices with knowledge of the private key.

WEP has been shown to be vulnerable to passive attacks, and is therefore considered inadequate if used alone. However, WEP is still useful as a minimal deterrent because it prevents a casual hacker from quickly accessing the wireless network.

MAC Address Access Control Lists (ACLs)

In a Tropos network, DHCP address assignment is used to enable end-user devices and network elements to communicate. To prevent unauthorized client devices and Wi-Fi cells from accessing the network, DHCP servers can be configured with a specific list of authorized MAC addresses (and optionally, their address assignments).

If a MAC ACL is employed, clients and Wi-Fi cells will be assigned an IP address only if the MAC address of their 802.11b radio is present in the list. Requests for IP addresses from devices with MAC addresses not on the list are an indication of unauthorized intrusion attempts. Those clients and Wi-Fi cells will be denied access to the wireless LAN.

MAC address ACLs are a form of **network access control** and should be considered as an additional layer of security that can be used in conjunction with layer 2 security.

DHCP is an IETF standard protocol which sends messages in the clear (i.e., unencrypted). Because sophisticated hackers can "spoof" the hardware address of a valid

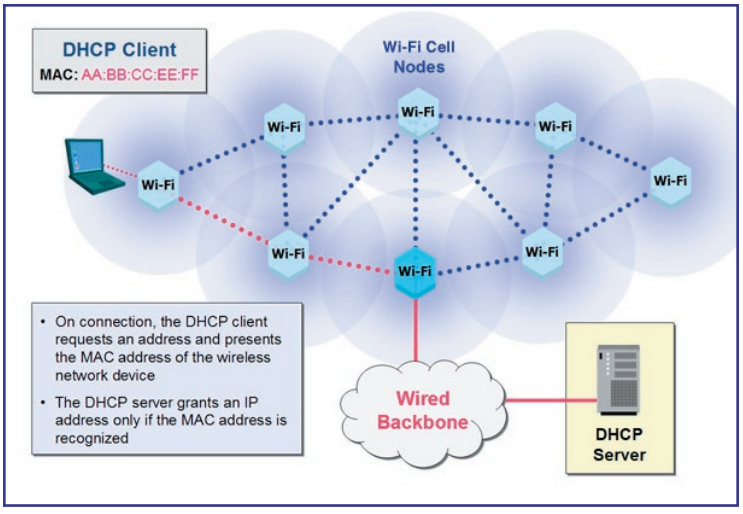


Figure 2: MAC Address Filtering

computer, MAC address-based authentication can only be considered one more element of the layered architecture designed to minimally deter casual hackers from easily gaining access to the wireless LAN.

WEP and MAC address ACLs can be considered minimal deterrents. They offer a limited amount of security, the techniques to overcome them are fairly well known, and they require a modest amount of expertise and/or computational resources to circumvent.

While Tropos employs both methods, to implement basic network access control and secure data transmission, they are minimal deterrents, primarily useful as the first step in a comprehensive wireless security strategy, and cannot be relied upon to protect sensitive data.

ESSID Suppression

Wi-Fi cells broadcast their ESSID (their network name) in the same manner as other forms of Wi-Fi infrastructure devices. For networks where public access is desired, this is an essential function, altering potential users of the network's availability in a particular area and allowing them to choose to connect. However, for private networks, that is, networks where access is limited to a specified set of users who already know of its existence, ESSID broadcast opens a potential security hole because it announces the network's availability to unauthorized persons.

Tropos Wi-Fi cells allow network administrators to optionally suppress ESSID broadcasts. In a private network, this does not hamper user access because client devices can be configured to attach to the network even is the ESSID is suppressed. Suppressing the ESSID broadcasts means that unauthorized persons will not even know the network is available unless they use sophisticated sniffing tools.

Like other Layer 2 security mechanisms, ESSID suppression has been shown to be vulnerable to passive attacks, and is therefore considered inadequate if used alone. However, it is useful as a minimal deterrent because it prevents a casual hacker from quickly accessing the wireless network.

Layer 3 and Layer 4 Techniques: Address, Protocol and TCP Port Filtering

Packet filtering firewalls have long been used in conventional wired network security architectures. Tropos has extended the concept to 802.11b, with its implementation of Layer 3 and 4 packet filtering. When these techniques are used in conjunction with WEP and MAC address ACLs, the wireless network no longer is the weak link in the security chain.

Tropos Wi-Fi cells can filter traffic at the edge of the wireless networks, using filters based on IP source and destination addresses, protocol and TCP port. For instance, if wireless access is permitted only for a specific set of clients for web browsing and e-mail, only traffic matching that profile will be forwarded by the Tropos Wi-Fi cells. That is, only traffic from defined IP addresses or subnets destined to defined IP addresses or subnets using a defined TCP port e.g., TCP port 80 for HTTP, port 110 for POP3 will be forwarded.

This capability brings a new dimension to 802.11b networks. Filters can be crafted that will disallow traffic to unprotected wired or wireless hosts, and the policies will be enforced at the very edge of the wireless network.

These security measures contribute to four aspects of wireless security, **network access control, protection of wired assets, protection of wireless clients** and **secure configuration and management**.

Layer 7 Security: VPNs Combined with Layers 3 and 4 Filtering

To provide industry-leading security, Tropos Networks recommends and uses techniques that provide strong security measures. These measures are very challenging or impossible to overcome even when attacked by serious and sophisticated adversaries. Building on the lower layer methods we've already discussed, Tropos Wi-Fi cells combine unique VPN compatibility and traffic filtering with industry-tested VPN encryption to offer the highest levels of security in 802.11 wireless networking.

As enterprises began allowing employees to connect to internal networks via the Internet, virtual private networks (VPNs) were developed in response to the security threats posed by malicious hackers attempting to gain access to internal network resources. Connections from the Internet to the internal network are encrypted by the VPN once the user requesting the connection authenticates successfully. Other incoming connections are disallowed. Driven by the increasing popularity of remote corporate access over Internet links, VPNs have rapidly matured over the past several years.

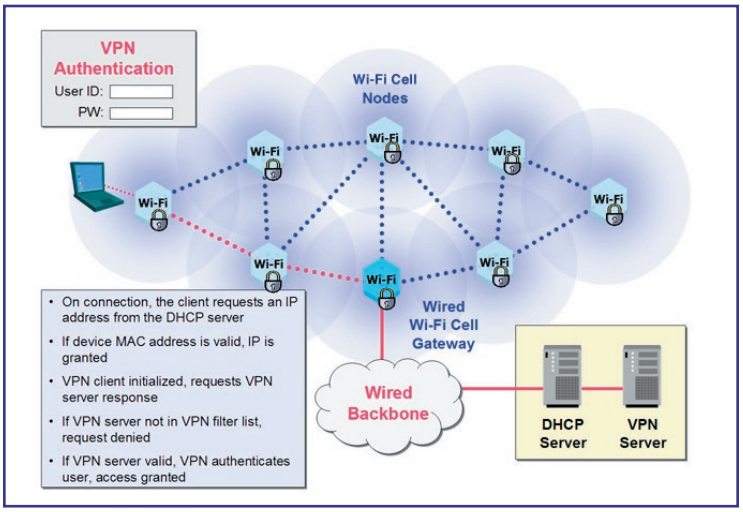


Figure 3: Tropos VPN Support and Filtering

Today, connecting wireless networks to an existing wireline network poses risks similar those encountered when first connecting to internal networks via the Internet. Because wireless signals propagate far beyond the physical confines of the typical data network, wireless connections to the wired network also become a potential access method that can be exploited by malicious hackers.

Because of this threat, Tropos Networks strongly recommends using VPN when using cellular Wi-Fi networks to connect to any organization's internal network. VPNs (typically based on IPSec) are available from numerous vendors and offer proven implementations of **network access control** and **secure data transmission.** Tropos Wi-Fi cells have demonstrated compatibility with a number of commercially available VPNs, including those from Cisco, PadCom and NetMotion.

Tropos Wi-Fi cells use traffic filtering to enhance the security provided by VPNs. Packet filters on all Wi-Fi cells can limit traffic on the wireless network to VPN traffic and other necessary protocols destined for authorized VPN servers on the wireline network. These measures **protect wired assets** by insulating wired assets from the wireless network and **protect wireless clients** by not allowing traffic to be directed to them.

Control Plane Security

In addition to securing data transmission, it is also crucial to secure the control and management of the network infrastructure.

Tropos Lightweight Control Protocol

Tropos Wi-Fi cells uses strong security measures to protect the protocol used by the Wi-Fi cells to transmit node identification and path selection information to each other.

These network elements communicate with each other only using UDP payloads encrypted with 128-bit AES. AES is the successor to DES and is recommended by the United States National Institute of Standards and Technology (NIST) as the most robust private key encryption technique.

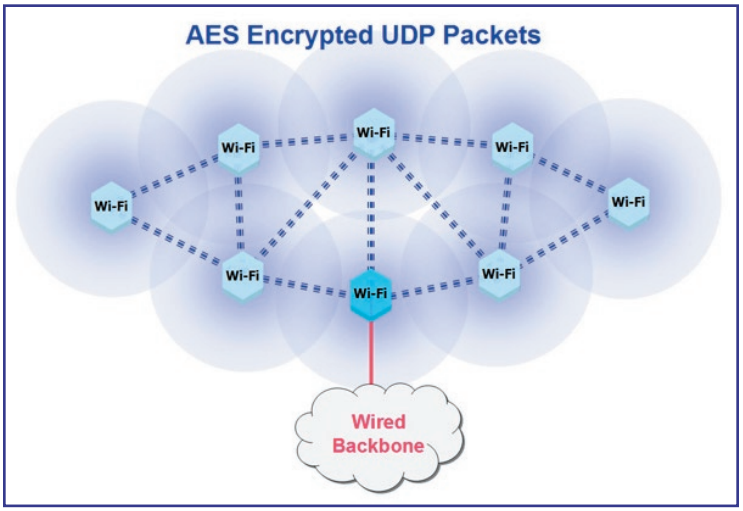


Figure 4: Tropos Control Protocol

Management Traffic Encryption

Metro-scale Wi-Fi networks constructed using Tropos Wi-Fi cells can be managed using an element manager, Tropos Control. Tropos Control uses a proxy architecture, in which Wi-Fi cells configured as gateways collect management information from associated nodes, and send it, using SNMP, to a management server. Because transmission from nodes to their associated gateway traverse wireless links, Tropos encrypts this traffic using AES, protecting it from unauthorized snooping.

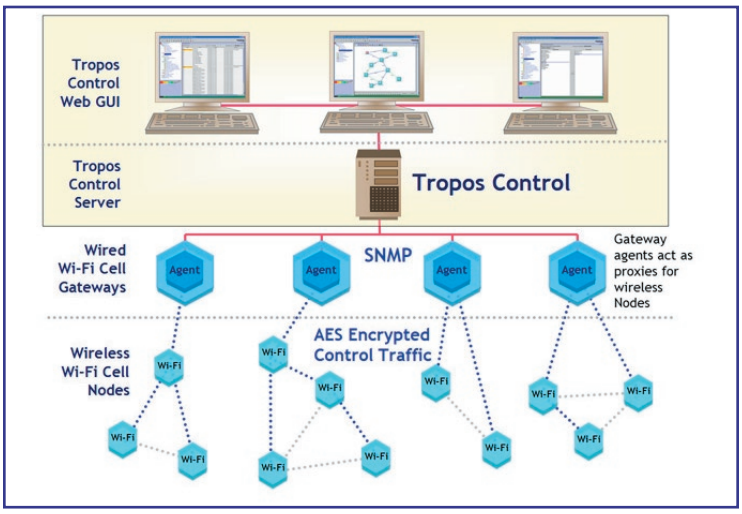


Figure 5: Tropos Control EMS

Secure Wi-Fi Cell Configuration

In addition to the Tropos Control element manager, Tropos Wi-Fi cells can be configured and monitored by a web-based configurator. All configurator traffic is protected with HTTPS (see Figure 5). Network administrators can securely monitor and configure individual Wi-Fi cells from anywhere on the Internet.

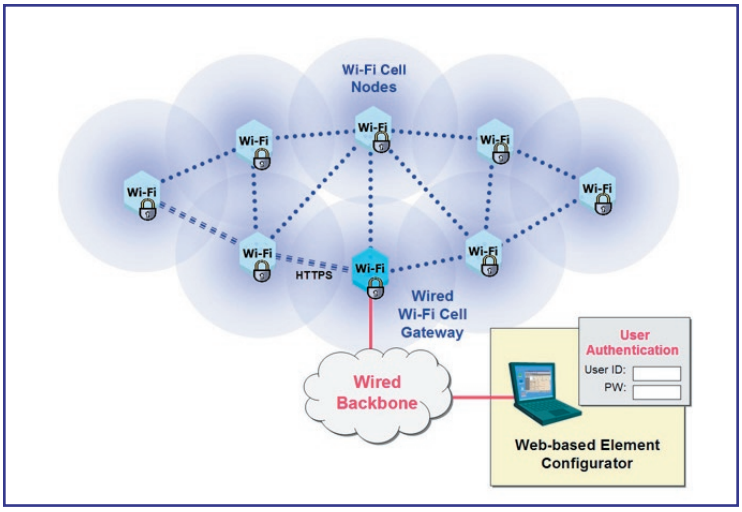


Figure 6: Secure Configuration

These techniques combine to enable **secure configuration and management** by preventing unauthorized access to, or monitoring of, the network's management and control traffic by malicious third-parties.

Summary

By leveraging the inherent intelligence of its Wi-Fi cells, Tropos combines the most rigorous Internet security techniques to offer a robust and multi-layered security framework.

This security framework can be configured to suit a broad range of access strategies, from the relatively unrestricted public access with minimal deterrents required by a wireless ISP, to the totally secure private network needed for law enforcement and public safety applications.

Using this multi-layer approach, network administrators have at least two tools they can choose to use to secure each of the five main areas of concern in wireless networks.

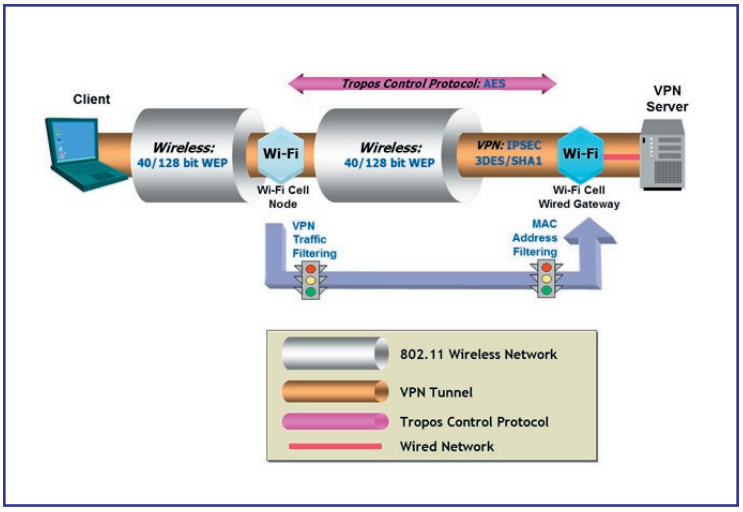
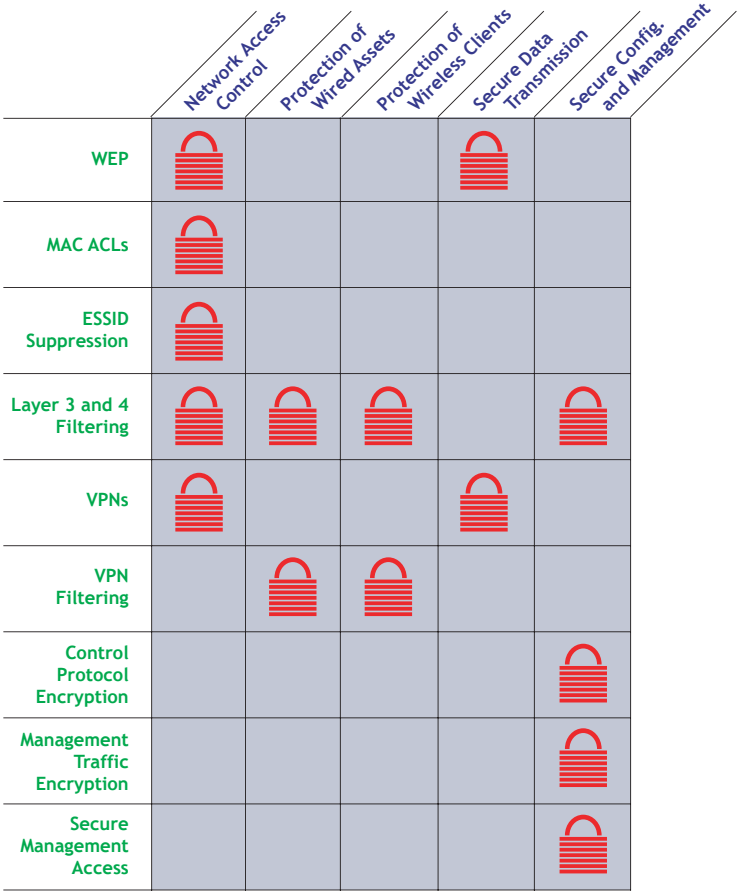


Figure 6: Tropos Multi-Layer Security Architecture



A final advantage of the Tropos security approach it upgradeability.

New security threats are constantly emerging and new techniques for combating threats are continually evolving. Because Tropos Wi-Fi cells are very intelligent, and most security features are implemented in software, Wi-fi cells' security features can be upgraded with new releases of Tropos Sphere, the Tropos network operating system. For example, ESSID suppression was a new feature in Tropos Sphere 2.0.

In the future, additional security features will be added to Tropos Sphere. Among the features being considered for future addition are WPA, 802.1x, VLANs, Radius and encryption for DHCP.

The upgradeability of Tropos Wi-Fi cells ensures that Tropos metro-scale Wi-Fi networks will remain as secure in the future as they are today and that users will reap the benefits of increasing levels of functionality.

1710 South Amphlett Blvd, Suite 304
San Mateo, CA 94402
T 650.286.4250
F 650.286.4259
@ sales@tropos.com
W www.tropos.com